Inhaltsverzeichnis

Einführung

Willkommen bei *Blockchain für Dummies*! Dies ist genau das richtige Buch für Sie, wenn Sie mehr darüber erfahren wollen, was Blockchains sind und wie man sie verwendet. Viele Menschen vermuten, Blockchains seien schwer zu verstehen. Vielleicht denken auch Sie, dass Blockchains einfach irgendwelche Kryptowährungen sind wie beispielsweise Bitcoin – aber tatsächlich sind sie sehr viel mehr. Jeder kann die Grundlagen für das Blockchain-System verstehen.

In diesem Buch finden Sie viele praktische Hinweise, wie Sie sich in der Blockchain-Welt bewegen können, und ebenso zu den Kryptowährungen, die darin geschaffen werden. Außerdem finden Sie nützliche Schritt-für-Schritt-Anleitungen, anhand derer Sie verstehen, wie Blockchains funktionieren und wo sie nützlich sind. Sie brauchen keinerlei Hintergrundwissen im Hinblick auf Programmierung, Wirtschaft oder Weltgeschehen, um dieses Buch verstehen zu können. Es wird jedoch immer wieder um diese Themen gehen, weil die Blockchain-Technologie mit all diesen Themen Überschneidungen hat.

Über dieses Buch

Dieses Buch erklärt Ihnen die Grundlagen, die Sie brauchen, um Blockchains, Smart Contracts und Kryptowährungen zu verstehen. Wahrscheinlich haben Sie sich dieses Buch gekauft, weil Sie schon viel über Blockchains gehört haben, wissen, dass sie wichtig sind, aber keine Ahnung haben, worum es sich dabei handelt, wie sie funktionieren oder wie Sie damit umgehen sollten. Auf den folgenden Seiten finden Sie leicht verständliche Antworten auf all diese Fragen.

Dieses Buch unterscheidet sich von allen anderen Büchern über Blockchains auf dem Markt: Es zeigt Ihnen die wichtigsten Blockchains auf dem öffentlichen Markt und erklärt, wie sie funktionieren, was sie leisten und was Sie heute Sinnvolles damit tun können.

Darüber hinaus beschäftigt sich dieses Buch auch mit der Welt der Blockchain-Technologie und erläutert Ihnen, was Sie bei Ihren eigenen Blockchain-Projekten beachten müssen. Hier erfahren Sie, wie Sie ein Ethereum-Wallet installieren, einen Smart Contract erstellen und ausfertigen, Einträge in Bitcoin und Factom vornehmen und Kryptowährungen verdienen.

Wenn Sie schon ein bisschen Erfahrung und etwas Wissen über Blockchains haben, brauchen Sie das Buch nicht von vorne nach hinten zu lesen. Blättern Sie einfach zu dem Thema, das Sie gerade am meisten interessiert. Wenn Sie ein Neuling sind, empfiehlt es sich allerdings schon, das Buch wie einen Roman zu lesen: vorne anzufangen und so lange zu lesen, wie Sie das Buch interessiert. Idealerweise natürlich bis zum Ende.

Manchmal finden Sie in diesem Buch Webadressen, die über zwei Textzeilen umbrochen sind. Wenn Sie dieses Buch auf Papier lesen und eine dieser Webseiten besuchen wollen, geben Sie sie einfach genauso ein, wie sie im Text dargestellt werden, so als ob der Zeilenumbruch gar

nicht existieren würde. Und wenn Sie den Text als E-Book lesen, haben Sie es ohnehin ganz einfach – Sie klicken einfach auf die Webadresse und gelangen direkt auf die Webseite.

Törichte Annahmen über den Leser

Sie brauchen nichts über Kryptowährungen, Programmierung und rechtliche Angelegenheiten zu wissen, aber ich setze das Folgende voraus:

- ✔ Sie haben einen Computer und Zugriff auf das Internet.
- ✔ Sie wissen, wie der Computer und das Internet genutzt werden.
- ✔ Sie wissen, wie Sie sich mithilfe von Menüs in Programmen bewegen.
- ✔ Blockchains sind Ihnen neu und Sie sind kein erfahrener Programmierer. Aber auch als Programmierer können Sie in diesem Buch viel lernen – vielleicht können Sie jedoch einige der Schritt-für-Schritt-Anleitungen überspringen.

Symbole in diesem Buch

In diesem Buch verwende ich Symbole, um Ihre Aufmerksamkeit auf bestimmte Arten von Informationen zu lenken. Und das bedeuten diese Symbole:

Das Tipp-Symbol kennzeichnet Tipps und Lösungen, die Ihnen das Leben mit Blockchains erleichtern.

Das Erinnerungssymbol kennzeichnet Informationen, die Sie unbedingt kennen sollten – alles, was Sie sich merken sollten. Um sich schnell einen Überblick über die wichtigsten Informationen eines Kapitels zu verschaffen, suchen Sie einfach nach diesen Symbolen.

Das Techniker-Symbol kennzeichnet höchst technische Inhalte, die Sie überspringen können, ohne das Wesentliche des jeweiligen Themas zu verpassen.

Das Warnsymbol weist darauf hin, dass Sie aufpassen sollten! Es kennzeichnet wichtige Informationen, die Ihnen Kopfzerbrechen ersparen – oder Token.

Wie es von hier aus weitergeht

Sie können die Blockchain-Technologie in fast jeder Branche einsetzen. Derzeit ist ein explosionsartiges Wachstum in den Bereichen Finanzen, Gesundheitswesen, Regierung und Versicherungen zu beobachten – und das ist erst der Anfang. Die ganze Welt befindet sich im Wandel und es gibt endlose Möglichkeiten.

Teil I
Erste Schritte mit Blockchains

IN DIESEM TEIL ...

Erfahren Sie, was Blockchains überhaupt sind und wie Ihr Unternehmen davon profitieren kann.

Identifizieren Sie die richtige Technologie für sich und lernen, wie Sie in vier Schritten ein effektives Blockchain-Projekt entwickeln und ausführen.

Erstellen Sie Ihre eigenen Smart Contracts auf Bitcoin und stellen fest, wo in Ihrem Unternehmen diese Technologie von Nutzen sein kann.

Entdecken Sie die Tools, die Sie benötigen, um Ihre eigene private Blockchain auf Ethereum einzurichten und auszuführen.

IN DIESEM KAPITEL

- Die neue Welt der Blockchains kennenlernen
- Verstehen, warum Blockchains so wichtig sind
- Die drei Typen von Blockchains identifizieren
- Ihre Kenntnisse über die Arbeitsweise von Blockchains vertiefen

Kapitel 1
Blockchain – eine Einführung

Ursprünglich war *Blockchain* in der Informatik der Begriff für eine bestimmte Art der Strukturierung und Weitergabe von Daten. Heute werden Blockchains als die »fünfte Evolution« der Programmierung bejubelt.

Blockchains sind ein neuer Ansatz für verteilte Datenbanken. Die eigentliche Innovation ergibt sich dadurch, dass alte Technologie auf neue Weise eingesetzt wird. Sie können sich Blockchains als verteilte Datenbanken vorstellen, die von einer bestimmten Personengruppe kontrolliert werden und in denen Informationen gespeichert und geteilt werden.

Es gibt viele verschiedene Arten von Blockchains und Blockchain-Anwendungen. Blockchains sind eine allumfassende Technologie, die plattform- und hardwareübergreifend auf der ganzen Welt eingesetzt wird.

Von Anfang an: Was sind Blockchains?

Eine Blockchain ist eine Datenstruktur, die es ermöglicht, eine Art digitales Kontenbuch (das sogenannte »Ledger«) mit Daten zu erstellen und es über ein Netzwerk unabhängiger Parteien zu teilen. Es gibt verschiedene Typen von Blockchains:

- ✔ **Öffentliche Blockchains**: Öffentliche Blockchains, wie beispielsweise Bitcoin, sind große verteilte Netzwerke, die unter Verwendung eines eigenen spezifischen Tokens arbeiten. Sie sind für alle Benutzer auf allen Ebenen geöffnet und verwenden Open-Source-Code, den ihre Community pflegt.
- ✔ **Permissioned Blockchains**: Permissioned Blockchains, wie beispielsweise Ripple, steuern die Rollen, die einzelne Teilnehmer innerhalb des Netzwerks übernehmen können. Es handelt sich ebenfalls um große und verteilte Systeme, die ein natives Token verwenden. Ihr Kerncode kann Open Source sein, muss aber nicht.

- ✔ **Private Blockchains**: Private Blockchains sind im Allgemeinen kleiner und verwenden kein Token. Die Mitgliedschaft wird streng kontrolliert. Diese Art Blockchains werden von Gruppen favorisiert, die zuverlässige Mitglieder haben und vertrauliche Informationen weitergeben.

Alle drei Blockchain-Typen setzen die Kryptografie ein, um einem Teilnehmer in einem bestimmten Netzwerk zu gestatten, den Ledger (das Kontobuch) sicher zu verwalten, ohne dass eine zentrale Autorität die Regeln durchsetzt. Der Wegfall dieser zentralen Autorität aus der Datenbankstruktur ist eine der wichtigsten und leistungsstärksten Eigenschaften von Blockchains.

Blockchains erstellen permanente Aufzeichnungen und Verläufe von Transaktionen, aber nichts ist wirklich uneingeschränkt permanent. Die Permanenz des Datensatzes basiert auf der Permanenz des Netzwerks. Im Kontext von Blockchains bedeutet das, dass ein großer Teil einer Blockchain-Community sich darauf einigen müsste, die Informationen zu ändern, und es besteht ein Anreiz, die Daten *nicht* zu ändern.

Wenn Daten in einer Blockchain aufgezeichnet werden, ist es extrem schwierig, sie zu ändern oder zu entfernen. Wenn jemand einer Blockchain einen Datensatz hinzufügen will, auch als Transaktion oder Eintrag bezeichnet, überprüfen Netzwerk-Benutzer, die die Validierungskontrolle besitzen, die vorgeschlagene Transaktion. Und hier wird das Ganze unübersichtlich, weil jede Blockchain eine leicht unterschiedliche Vorstellung davon hat, wie das passieren soll und wer eine Transaktion validieren kann.

Was Blockchains können

Eine Blockchain ist ein Peer-to-Peer-System ohne zentrale Autorität, die den Datenstrom verwaltet. Eine grundlegende Möglichkeit, die zentrale Kontrolle wegfallen zu lassen und gleichzeitig die Datenintegrität zu bewahren, ist ein großes verteiltes Netzwerk unabhängiger Benutzer. Das bedeutet, dass sich die Computer, aus denen sich das Netzwerk zusammensetzt, an unterschiedlichen Orten befinden. Solche Computer werden häufig auch als *vollständige Knoten* bezeichnet.

Abbildung 1.1 zeigt die Struktur des Blockchain-Netzwerks Bitcoin. In Aktion sehen Sie das Ganze unter `http://dailyblockchain.github.io`.

Um zu verhindern, dass das Netzwerk beschädigt wird, werden die Blockchains nicht nur dezentralisiert, sondern sie verwenden auch häufig eine eigene Kryptowährung. Eine *Kryptowährung* ist ein digitales Token mit einem bestimmten Marktwert. Kryptowährungen werden an Börsen ähnlich wie Aktien gehandelt.

Kryptowährungen verhalten sich für jede Blockchain etwas anders. Grundsätzlich zahlt die Software dafür, dass die Hardware betrieben wird. Die Software ist das Blockchain-Protokoll. Bekannte Blockchain-Protokolle sind unter anderem Bitcoin, Ethereum, Ripple, Hyperledger oder Factom. Die Hardware besteht aus den vollständigen Knoten, die die Daten im Netzwerk sichern.

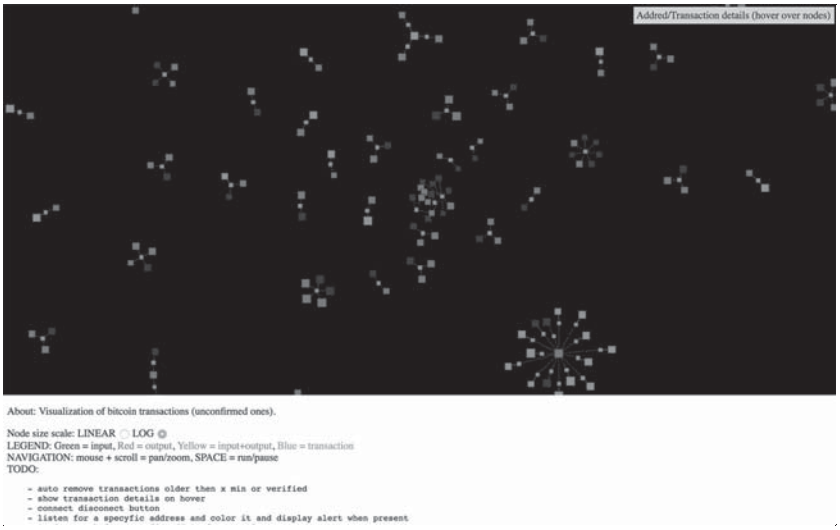

Abbildung 1.1: Der Aufbau des Blockchain-Netzwerks Bitcoin

Warum Blockchains so wichtig sind

Blockchains werden heute als die »fünfte Evolution« der Programmierung betrachtet – die bisher fehlende Vertrauensschicht im Internet. Dies ist einer der Gründe, warum sich so viele Menschen für dieses Thema interessieren.

Blockchains können Vertrauen in digitale Daten schaffen. Wenn Informationen in eine Blockchain-Datenbank geschrieben wurden, ist es so gut wie unmöglich, sie zu entfernen oder zu ändern. Diese Möglichkeit hat nie zuvor existiert.

Wenn Daten permanent und zuverlässig in einem digitalen Format vorliegen, können Sie Geschäfte online erledigen, die in der Vergangenheit nur offline getätigt werden konnten. Alles, was bisher analog war, unter anderem Eigentumsrechte und Identitäten, kann jetzt online erstellt und verwaltet werden. Langsame Unternehmens- und Bankenprozesse wie Geldüberweisungen und Fondsabwicklungen können heute fast unmittelbar erledigt werden. Die Möglichkeiten, die sich durch sichere digitale Aufzeichnungen ergeben, sind von größter Bedeutung für die Weltwirtschaft.

Die ersten Anwendungen waren so ausgelegt, dass sie sich auf die sichere digitale Übertragung von Vermögenswerten stützten, die Blockchains durch den Austausch ihrer nativen Token ermöglichten. Dabei ging es unter anderem um die Überweisung von Geld und Kapital. Die Möglichkeiten der Blockchain-Netzwerke gehen jedoch weit über die Verschiebung von Vermögenswerten hinaus.

Aufbau von Blockchains

Blockchains setzen sich aus drei Kernkomponenten zusammen:

- ✔ **Block**: Eine Liste mit Transaktionen, die über einen bestimmten Zeitraum in einem Ledger (»Kontobuch«) aufgezeichnet werden. Die Größe, der Zeitraum und das auslösende Ereignis unterscheiden sich zwischen allen Blockchains.
  Nicht alle Blockchains haben das primäre Ziel, einen Datensatz über eine Bewegung ihrer Kryptowährung aufzuzeichnen und zu sichern, aber alle Blockchains zeichnen die Bewegung ihrer Kryptowährung oder ihres Tokens auf. Sie können sich eine *Transaktion* einfach als die Aufzeichnung von Daten vorstellen. Durch die Zuweisung eines Werts (wie es beispielsweise in einer Finanztransaktion geschieht) wird interpretiert, was diese Daten bedeuten.

- ✔ **Kette (»Chain«)**: Ein Hash-Schlüssel, der die Blöcke verknüpft, sie mathematisch »verkettet«. Dies ist eines der anspruchsvollsten Blockchain-Konzepte und nicht so einfach zu verstehen. Aber genau dieser scheinbar magische Mechanismus verbindet die Blockchains fest miteinander und ermöglicht mathematisch gestütztes Vertrauen.
  Der Hash-Schlüssel in Blockchains wird aus den Daten des jeweils vorhergehenden Blocks erzeugt. Es handelt sich um einen Fingerabdruck dieser Daten, der ihre Reihenfolge und Uhrzeit unveränderbar festschreibt.

  Blockchains sind relativ neu – das Hashing nicht: Es wurde bereits vor über 30 Jahren erfunden. Diese betagte Technik wird deshalb verwendet, weil sie eine nicht entschlüsselbare Einwegfunktion schafft. Eine Hash-Funktion erzeugt einen mathematischen Algorithmus, der Daten beliebiger Größe auf einen Bit-String fester Größe abbildet. Ein Bit-String ist normalerweise 32 Zeichen lang und repräsentiert die Daten, für die das Hashing durchgeführt wurde. Der Secure Hash Algorithm (SHA) ist eine von mehreren verschlüsselnden Hash-Funktionen, die in Blockchains verwendet werden. Ein gebräuchlicher Algorithmus ist SHA-256, der einen nahezu eindeutigen Hash-Schlüssel fester Größe (256 Bit, 32 Byte) erzeugt. Praktisch können Sie sich einen Hash-Schlüssel als digitalen Fingerabdruck von Daten vorstellen, mit dem diese innerhalb der Blockchain an einer festen Position gehalten werden.

- ✔ **Netzwerk**: Das Netzwerk setzt sich aus »vollständigen Knoten« zusammen. Sie können sich das so vorstellen, dass der Computer einen Algorithmus ausführt, der das Netzwerk sichert. Jeder Knoten enthält eine vollständige Aufzeichnung aller Transaktionen, die je in dieser Blockchain aufgezeichnet wurden.
  Die Knoten befinden sich auf der ganzen Welt und können von jedermann betrieben werden. Es ist schwierig, teuer und zeitaufwendig, einen vollständigen Knoten zu betreiben, deshalb machen es die Betreiber nicht kostenlos. Der Anreiz für den Betrieb eines Knotens besteht darin, Kryptowährung zu verdienen. Der zugrunde liegende Blockchain-Algorithmus belohnt sie für ihre Dienste. Diese Belohnung ist üblicherweise ein Token oder eine Kryptowährung wie Bitcoin.

Die Begriffe *Bitcoin* und *Blockchain* werden häufig synonym verwendet, bedeuten aber nicht dasselbe. Bitcoin hat eine Blockchain. Die Bitcoin-Blockchain ist das Protokoll, das die sichere Übertragung von Bitcoins ermöglicht. Der Begriff Bitcoin ist der Name der Kryptowährung, auf der das Bitcoin-Netzwerk basiert. Die Blockchain ist eine Software, Bitcoin ist eine spezifische Kryptowährung.

Blockchain-Anwendungen

Blockchain-Anwendungen sind um die Idee herum aufgebaut, dass das Netzwerk der Vermittler ist. Ein solches System ist eine unerbittliche und blinde Umgebung. Computercode wird zum Gesetz und die Regeln werden vom Netzwerk unveränderbar interpretiert und ausgeführt. Computer haben nicht die sozialen Tendenzen und Verhaltensweisen wie Menschen.

Das Netzwerk kann keine Absicht interpretieren (zumindest noch nicht). Als Anwendungsfall, der um diese Idee herum aufgebaut wurde, wurden über eine Blockchain vermittelte Versicherungsverträge weitreichend untersucht.

Eine weitere interessante Möglichkeit der Blockchains ist eine absolut unfehlbare Datenhaltung. Blockchains können eine unmissverständliche Zeitleiste erzeugen, die aufzeichnet, wer was und wann gemacht hat. Viele Branchen und Aufsichtsbehörden haben zahllose Stunden darauf verwendet, dieses Problem zu bewerten. Durch Blockchain-gestützte Aufzeichnungen fallen einige Schwierigkeiten bei der Interpretation vergangener Geschehnisse weg.

Der Blockchain-Lebenszyklus

Blockchains wurden mit Bitcoin eingeführt. Dabei zeigte sich, dass Einzelpersonen, die sich nie zuvor gesehen hatten, online innerhalb eines Systems arbeiten konnten, in dem es unmöglich war, andere Netzwerkteilnehmer zu betrügen.

Das ursprüngliche Bitcoin-Netzwerk sollte die Kryptowährung Bitcoin sichern. Es besteht aus ca. 5000 vollständigen Knoten, ist über die gesamte Welt verteilt und wird hauptsächlich für den Handel von Bitcoin und den Austausch von Vermögenswerten verwendet. Die Community erkannte jedoch das viel weiter reichende Potenzial des Netzwerks. Wegen seiner Größe und lange erprobten Sicherheit wird es auch zur Absicherung anderer, kleinerer Blockchains und Blockchain-Anwendungen verwendet.

Das Ethereum-Netzwerk ist eine zweite Weiterentwicklung des Blockchain-Konzepts. Hierbei wird die herkömmliche Blockchain-Struktur um eine Programmiersprache ergänzt. Wie Bitcoin verfügt das Ethereum-Netzwerk über 5000 vollständige Knoten und ist weltweit verteilt. Ethereum wird in erster Linie verwendet, um Ether zu handeln, Smart Contracts abzuschließen und DAOs (Dezentrale Autonome Organisationen) zu erstellen. Außerdem werden mit ihm Blockchain-Anwendungen und kleinere Blockchains abgesichert.

Das Factom-Netzwerk ist die dritte Weiterentwicklung der Blockchain-Technologie. Es verwendet ein weniger strenges Konsenssystem, unterstützt Abstimmungen und speichert sehr

viel mehr Informationen. Ursprünglich soll es hauptsächlich Daten und Systeme sichern. Factom arbeitet mit mehreren zu einem Bund vereinigten Knoten und einer unbegrenzten Anzahl an Prüfknoten. Das Netzwerk ist klein und verankert sich selbst in anderen verteilten Netzwerken, womit Brücken über die Blockchains entstehen.

Konsens: Die treibende Kraft der Blockchains

Blockchains sind leistungsstarke Tools, weil sie ehrliche Systeme schaffen, die selbstkorrigierend sind, ohne dass eine dritte Partei diese Regeln erzwingen muss. Die Regeln werden durch ihren Konsensalgorithmus erzwungen.

In der Blockchain-Welt ist *Konsens* der Prozess, eine Einigung innerhalb einer Gruppe grundsätzlich misstrauischer Teilnehmer zu erzielen. Diese Teilnehmer sind die vollständigen Knoten des Netzwerks. Die vollständigen Knoten werten die in das Netzwerk eingegebenen Transaktionen daraufhin aus, ob sie als Teil des Ledgers aufgezeichnet werden sollen.

Abbildung 1.2 zeigt, wie Blockchains eine Einigung erzielen.

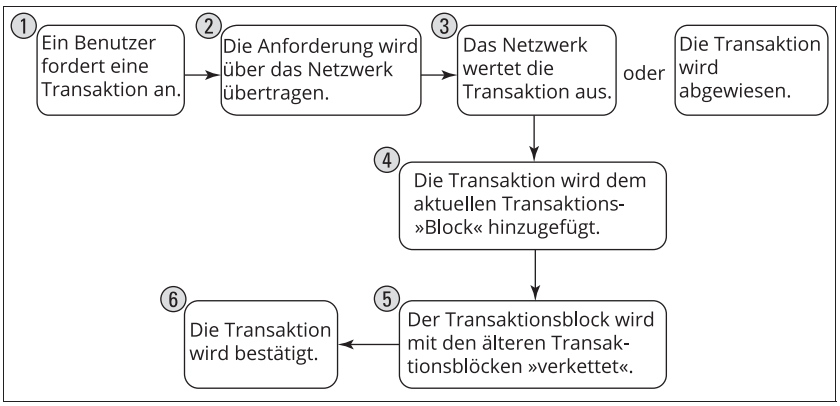

Abbildung 1.2: Wie Blockchains arbeiten

Jede Blockchain hat ihre eigenen Algorithmen, um eine Einigung über die hinzugefügten Einträge innerhalb ihres Netzwerks zu finden. Es gibt viele verschiedene Modelle, Konsens zu erzielen, weil jede Blockchain andere Einträge erzeugt. Einige Blockchains handeln Vermögenswerte, andere speichern Daten, wieder andere sichern Systeme und Verträge.

Bitcoin beispielsweise handelt den Wert seines Tokens zwischen den Mitgliedern in seinem Netzwerk. Die Token haben einen Marktwert, die Anforderungen im Hinblick auf Leistung, Skalierbarkeit, Konsistenz, Angriffsmodell und Ausfallmodell sind deshalb höher. Bitcoin arbeitet unter der Annahme, dass ein böswilliger Angreifer den Verlauf der Handelstransaktionen verändern könnte, um Token zu stehlen. Bitcoin verhindert dies durch ein Konsensmodell, das auch als *Proof of Work* (POW) bezeichnet wird. Es löst das aus der Informatik und Mathematik bekannte Problem der byzantinischen Generäle: »Wie können Sie wissen, ob die

Informationen, die Sie gerade sehen, nicht intern oder extern verändert wurden?« Die Zuverlässigkeit von Daten ist ein großes Problem in der Informatik, weil es fast immer möglich ist, Daten zu verändern oder zu manipulieren.

Die meisten Blockchains arbeiten unter der Annahme, dass sie durch externe Kräfte oder die Benutzer des Systems angegriffen werden. Die erwartete Bedrohung und der Vertrauensgrad des Netzwerks in die Knoten, die die Blockchain betreiben, bestimmt die Art des Konsensalgorithmus, mit dem sie ihr Ledger (das »Kontobuch«) führen. Bitcoin und Ethereum beispielsweise gehen von einer sehr hohen Bedrohung aus und verwenden einen starken Konsensalgorithmus, das *Proof of Work*. In diesen Netzwerken gibt es kein Vertrauen.

Auf der anderen Seite des Spektrums können Blockchains, die Finanztransaktionen zwischen einander bekannten Parteien aufzeichnen sollen, einen leichteren und schnelleren Konsens verwenden. Hier ist es wichtiger, dass die Transaktionen schnell vonstattengehen. Proof of Work ist in diesem Zusammenhang zu langsam und zu teuer, weil es vergleichsweise wenige Teilnehmer im Netzwerk gibt und jede Transaktion unmittelbar abgeschlossen werden muss.

Blockchains in der Praxis

Heute gibt es Hunderte von Blockchains und Blockchain-Anwendungen. Die ganze Welt ist besessen von der Idee, Geld noch schneller zu bewegen, Verwaltungsaufgaben mithilfe eines verteilten Netzwerks zu lösen und sichere Anwendungen sowie sichere Hardware zu entwickeln.

An Kryptowährungsbörsen finden Sie viele dieser öffentlichen Blockchains vor. Abbildung 1.3 zeigt beispielsweise die Altcoin-Börse für Poloniex (`https://poloniex.com`), eine Handelsplattform für Kryptowährung.

Abbildung 1.3: Die Handelsplattform Altcoin

Blockchains dienen längst nicht mehr nur dem Handel von Marktwerten, sondern werden in den unterschiedlichsten Branchen eingesetzt. Sie schaffen eine neue Vertrauensschicht, die die Online-Arbeit so sicher macht, wie es nie zuvor möglich war.

Derzeitige Verwendungen für Blockchains

Die meisten Blockchain-Anwendungen werden heute eingesetzt, um Geld oder andere Vermögenswerte schnell und kostengünstig zu bewegen. Sie werden im Aktienhandel eingesetzt, zur Bezahlung von Mitarbeitern in anderen Ländern oder auch für den Währungstausch.

Blockchains werden auch als Teil eines Software-Sicherheitsstapels eingesetzt. Das US-Ministerium für innere Sicherheit hat sich in jüngster Zeit mit Blockchain-Software beschäftigt, die IoT-Geräte (IoT = Internet of Things, Internet der Dinge) sichert. Die IoT-Welt zieht den größten Nutzen aus dieser Innovation, weil sie sehr empfindlich gegenüber Manipulationen und Hacking ist. Darüber hinaus sind IoT-Geräte mittlerweile allgegenwärtig, weshalb Sicherheit ein immer dringenderes Thema wird. Zu den wichtigsten Beispielen gehören Krankenhaussysteme, selbstfahrende Autos und Sicherheitssysteme.

Eine weitere interessante Blockchain-Innovation sind DAOs (Dezentrale Autonome Organisationen). Diese Blockchain-Anwendungen stellen eine neue Möglichkeit dar, Unternehmen online zu organisieren. Mit DAOs wurden über das Ethereum-Netzwerk bereits Gelder automatisiert verwaltet und investiert.

Blockchain-Anwendungen der Zukunft

Mittlerweile werden größere und langfristigere Blockchain-Projekte erforscht, unter anderem behördliche Grundbuchsysteme, digitale Identität sowie die Sicherheit im internationalen Reiseverkehr.

Die Möglichkeiten einer Zukunft mit allgegenwärtigen Blockchains haben die Fantasie von Geschäftsleuten, Regierungen, politischen Gruppen und humanitären Einrichtungen auf der ganzen Welt angeregt. Länder wie England, Singapur und die Vereinigten Arabischen Emirate betrachten Blockchains als Möglichkeit zur Kostenreduktion, für neue Finanzinstrumente und saubere Datenaufzeichnungen. Es gibt dort eine aktive Investitionspolitik und Initiativen, die sich mit Blockchains beschäftigen.

Blockchains haben die Grundlage geschaffen, die Notwendigkeit des Vertrauens aus der Gleichung zu nehmen. Bislang war es eine große Sache, vorab »Vertrauen« zu erbitten. Mit Blockchains ist das kein Problem mehr. Außerdem kann die Infrastruktur, die die Vorgaben durchsetzt, wenn dieses Vertrauen gebrochen wird, weniger aufwendig gestaltet werden. Die Gesellschaft basiert zu einem guten Teil auf Vertrauen und der Durchsetzung von Regeln. Die sozialen und wirtschaftlichen Auswirkungen von Blockchain-Anwendungen können aber auch emotional und politisch polarisieren, weil sich dadurch die Strukturen wertbasierter und sozialer Transaktionen ändern.